



Aalborg Universitet

AALBORG UNIVERSITY  
DENMARK

## Two applications of the footprint (or -set) bound

*Estimation of generalized Hamming weights*

Geil, Hans Olav

*Publication date:*  
2006

*Document Version*  
Publisher's PDF, also known as Version of record

[Link to publication from Aalborg University](#)

*Citation for published version (APA):*

Geil, H. O. (2006). *Two applications of the footprint (or -set) bound: Estimation of generalized Hamming weights*. Poster presented at Workshop D1: Gröbner Bases in Cryptography, Coding Theory and Algebraic Combinatorics, Lenz, Austria.

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

### Take down policy

If you believe that this document breaches copyright please contact us at [vbn@aub.aau.dk](mailto:vbn@aub.aau.dk) providing details, and we will remove access to the work immediately and investigate your claim.

# Two applications of the footprint (or $\Delta$ -set) bound

## Estimation of generalized Hamming weights

Olav Geil, Aalborg University

Based on joint works with T. Høholdt and H. E. Andersen

### 1 The Footprint (or $\Delta$ -set) bound

**Definition 1** Let  $\prec$  be a monomial ordering on  $\mathcal{M}(X_1, \dots, X_m)$  and  $k$  a field. Given an ideal  $I \subseteq k[X_1, \dots, X_m]$  the set

$$\Delta_{\prec}(I) = \{M \in \mathcal{M}(X_1, \dots, X_m) \mid \text{there does not exist any } F \in I \text{ with } \text{lm}(F) = M\}$$

is called the footprint of  $I$

**Theorem 2** If  $\Delta_{\prec}(I)$  is finite then  $\#V_k(I) \leq \#\Delta_{\prec}(I)$  holds. Equality holds if  $I$  is radical. In particular  $\#V_k(I) = \#\Delta_{\prec}(I \cup \langle X_1^q - X_1, \dots, X_m^q - X_m \rangle)$ .

### 2 Generalized Hamming weights

**Definition 3** The  $i$ th generalized Hamming weight of a code  $C$  is

$$d_i(C) = \min\{\#\text{Sup}(U) \mid U \text{ is a linear subcode of } C \text{ of dimension } i\}$$

Let  $\{P_1, \dots, P_s\} = V_{\mathbb{F}_q}(\langle G_1, \dots, G_s \rangle)$  and  $\text{ev}(F) = (F(P_1), \dots, F(P_s))$ .

$$A = \begin{bmatrix} \text{ev}(F_1) \\ \vdots \\ \text{ev}(F_s) \end{bmatrix}$$

$$[F] = \{F_i + \sum_{j=1}^s \alpha_j F_j \mid \alpha_j \in \mathbb{F}_q\}$$

$$D_{\{[F_1], \dots, [F_s]\}} = \max\{\#\{P_j \in V \mid F'_i(P_j) = \dots = F'_s(P_j) = 0\} \mid F'_i \in [F_i], i = 1, \dots, s\}$$

$$D_i = \max\{D_{\{[F_1], \dots, [F_s]\}} \mid 1 \leq i_1 < \dots < i_s \leq r\}.$$

**Theorem 4** Let  $C$  be a code with parity check matrix  $A$  (not necessarily of full rank) then for  $d^* \leq a+t, t \leq k, d \leq n$  we have

$$d_t \geq d^* \Leftrightarrow D_{a-d^*+t+1} \leq d^* - 2$$

$$d_t \leq d^* \Leftrightarrow D_{a-d^*+t} \geq d^*$$

**Theorem 5** Let  $C$  be a code with generator matrix  $A$  (assumed to be of full rank) then for  $t = 1, \dots, k$  we have  $d_t = n - D_t$ .

**Observation 6**

$$D_{\{[F_1], \dots, [F_s]\}} = \max\{\#\Delta_{\prec}(\{F'_1, \dots, F'_s, G_1, \dots, G_s, X_1^q - X_1, \dots, X_m^q - X_m\} \mid F'_i \in [F_i], i = 1, \dots, s\}$$

$$\leq \#\Delta_{\prec}(\{\text{lm}(F_1), \dots, \text{lm}(F_s), G_1, \dots, G_s,$$

### 3 Weighted degree orderings

**Definition 7** Given weights  $w(X_1), \dots, w(X_m) \in \mathbb{R}_+$  define  $\prec_w$  on  $\mathcal{M}(X_1, \dots, X_m)$  by  $X_1^{i_1} \dots X_m^{i_m} \prec_w X_1^{j_1} \dots X_m^{j_m}$  if one of following conditions holds

- (1)  $w(X_1^{i_1} \dots X_m^{i_m}) < w(X_1^{j_1} \dots X_m^{j_m})$
- (2)  $w(X_1^{i_1} \dots X_m^{i_m}) = w(X_1^{j_1} \dots X_m^{j_m})$  and  $X_1^{i_1} \dots X_m^{i_m} \prec_{\text{lex}} X_1^{j_1} \dots X_m^{j_m}$

**Proposition 8** Define a weighted degree monomial ordering by the weights  $w(X) = b$  and  $w(Y) = a$  and consider

$$F(X, Y) = X^a + \alpha Y^b + F'(X, Y)$$

$$G(X, Y) = X^i Y^j + G'(X, Y)$$

where  $\alpha$  is non-zero and  $a, b > 0$ ,  $w(F') < ab$ , and  $w(G') < bi + aj$ . The equation set  $F(X, Y) = G(X, Y) = 0$  has at most  $bi + aj$  solutions

### 4 Parity check matrix description

**Improved Hermitian codes**

Let  $V$  be the 64 points on the Hermitian curve  $X^5 + Y^4 + Y$  over  $\mathbb{F}_{16}$ . Let parity check matrix be

$$\begin{bmatrix} \text{ev}(1) \\ \text{ev}(X) \\ \text{ev}(Y) \\ \text{ev}(X^2) \\ \text{ev}(XY) \\ \text{ev}(Y^2) \\ \text{ev}(X^3) \\ \text{ev}(Y + X^4) \end{bmatrix}$$

$D_{\{[XY], [Y + X^4]\}} \leq 7$  follows from Proposition 8

$D_{\{[Y^2], [Y^3 + X^4]\}} \leq 8$  follows by choosing  $w(X) = 1$  and  $w(Y) = 1.1$

$D_{\{[X], [X], [Y + X^4]\}} \leq 6$  follows by choosing  $w(X) = 1$  and  $w(Y) = 1.4$

Going through all combinations gives  $D_1 \leq 16, D_2 \leq 8, D_3 \leq 6$  and  $D_4 \leq 4$ .

This implies  $d_1 \geq 6, d_2 \geq 8, d_i \geq i + 7$  for  $i = 3, \dots, 9$  and  $d_i = i + 8$  for  $i = 10, \dots, 56$ . Not only minimum distance is improved.

### 5 Generator matrix description

**Hermitian codes over  $\mathbb{F}_{16}$**  Defining polynomial  $X^5 + Y^4 + Y$  has 64 zeros which gives an evaluation map  $\text{ev}: \mathbb{F}_{16}[X, Y] \rightarrow \mathbb{F}_{16}^{64}$ .

Choose  $w(X) = 5, w(Y) = 4$  and lexicographic ordering with  $X \prec_{\text{lex}} Y$ . By standard results

$$\text{ev}(\Delta_{\prec_w}((X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y)))$$

constitutes a basis for  $\mathbb{F}_{16}^{64}$ . Below is listed

$$\#(\Delta_{\prec_w}((X^i Y^j, X^5 + Y^4)) \cap \Delta_{\prec_w}((X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y)))$$

for all

$$X^i Y^j \in \Delta_{\prec_w}((X^5 + Y^4 + Y, X^{16} + X, Y^{16} + Y))$$

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 15 | 19 | 23 | 27 | 31 | 35 | 39 | 43 | 47 | 51 | 55 | 59 | 60 | 61 | 62 | 63 |
| 10 | 14 | 18 | 22 | 26 | 30 | 34 | 38 | 42 | 46 | 50 | 54 | 56 | 58 | 60 | 62 |
| 5  | 9  | 13 | 17 | 21 | 25 | 29 | 33 | 37 | 41 | 45 | 49 | 52 | 55 | 58 | 61 |
| 0  | 4  | 8  | 12 | 16 | 20 | 24 | 28 | 32 | 36 | 40 | 44 | 48 | 52 | 56 | 60 |

Traditional codes corresponds to linear span of all  $\text{ev}(X^i Y^j)$  with  $w(X^i Y^j) \leq s$ .

Improved codes corresponds to linear span of all  $\text{ev}(X^i Y^j)$  with  $\Delta$ -size at most some chosen number.

|             | k  | d <sub>1</sub> | d <sub>2</sub> | d <sub>3</sub> | d <sub>4</sub> | d <sub>5</sub> | d <sub>6</sub> | d <sub>7</sub> | d <sub>8</sub> | d <sub>9</sub> |
|-------------|----|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| Improved    | 55 | 6              | 8              | 9              | 11             | 12             | 14             | 15             | 16             | 18             |
| Traditional | 55 | 4              | 8              | 9              | 12             | 13             | 14             | 16             | 17             | 18             |
|             | k  | d <sub>1</sub> | d <sub>2</sub> | d <sub>3</sub> | d <sub>4</sub> | d <sub>5</sub> | d <sub>6</sub> | d <sub>7</sub> | d <sub>8</sub> | d <sub>9</sub> |
| Improved    | 51 | 9              | 12             | 14             | 15             | 17             | 18             | 19             | 21             | 21             |
| Traditional | 51 | 8              | 12             | 13             | 16             | 17             | 18             | 20             | 21             | 22             |
| Traditional | 50 | 9              | 13             | 14             | 17             | 18             | 19             | 21             | 21             | 22             |

Certainly, minimum distances are improved, but higher weights need NOT be.

### References

- [1] H. E. Andersen, On puncturing of codes from Norm-Trace curves, to appear in *Finite Fields and their Applications*.
- [2] A. I. Barbero and C. Munuera, The Weight Hierarchy of Hermitian Codes, *SIAM J. Discrete Math.*, **13**, 79-104.
- [3] D. Cox, J. Little and D. O'Shea, "Ideals, Varieties, and Algorithms, 2nd ed.," Springer, Berlin, 1997.
- [4] G.-L. Feng, T. R. N. Rao, G. A. Berg and J. Zhu, "Generalized Bezout's theorem in its applications in coding theory," *IEEE Trans. Inform. Theory*, **43**, 1799-1810.
- [5] O. Geil and T. Høholdt, "Footprints or Generalized Bezout's Theorem," *IEEE Trans. Inf. Theory*, **46**, 635-641.
- [6] O. Geil and T. Høholdt, On Hyperbolic Codes, Proc. AAECC-14, *Lecture Notes in Comput. Sci.* 2227, (S. Bozta, I. Spharlinkski, Eds.), Springer, Berlin, 2001, 159-171.
- [7] P. Heijnen and R. Pellikaan, Generalized Hamming Weights of q-ary Reed-Muller codes, *IEEE Trans. Inform. Theory*, **44**, (1998), 181-196